

UNIVERSIDADE DA CORUÑA

**LABORATORIO DE REDES:**  
**Tutorial de *Packet Tracer***



## Introducción

*Cisco Packet Tracer*<sup>1</sup> es un programa de simulación de redes que permite crear redes complejas y solucionar los mismos problemas que pueden surgir con dispositivos Cisco reales, pero sin la necesidad de disponer de dichos dispositivos. Este programa proporciona las características básicas que se pueden encontrar en el hardware Cisco real, aparte de otras funcionalidades como *VoIP*, *Wireless*, etc.

El objetivo de este tutorial es familiarizarse con el entorno de simulación. *Packet Tracer* dispone tanto de tutoriales como de ficheros de ayuda, que pueden ser de utilidad.

Se recomienda el empleo de la última versión (8.1.1) de *Packet Tracer*. Está disponible en <https://www.netacad.com/portal/resources/packet-tracer> o <https://skillsforall.com/resources/lab-downloads> tras registrarse. También os sugerimos la realización del curso accesible a través de la siguiente URL: <https://skillsforall.com/course/getting-started-cisco-packet-tracer>.

En la tabla 1 figuran los componentes de la interfaz de *Packet Tracer* marcados en la figura 1.

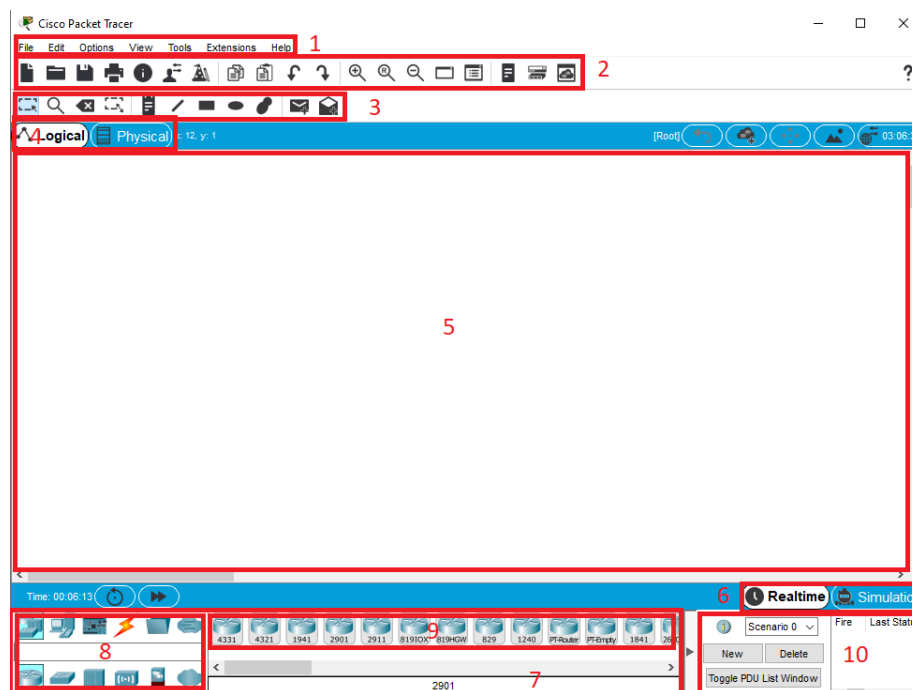


Figura 1: Interfaz de *Packet Tracer*

<sup>1</sup> [http://www.cisco.com/web/learning/netacad/course\\_catalog/PacketTracer.html](http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html)



Número	Nombre
1	Barra de menús
2	Barra de tareas principal
3	Barra de tareas comunes
4	<i>Workspace</i> físico/lógico y barra de navegación
5	<i>Workspace</i>
6	Barra <i>realtime</i> /simulación
7	Caja de componentes de red
8	Caja de selección del tipo de dispositivo
9	Caja de selección del dispositivo específico
10	Ventana de paquetes creados en los escenarios de simulación

Tabla 1: Componentes

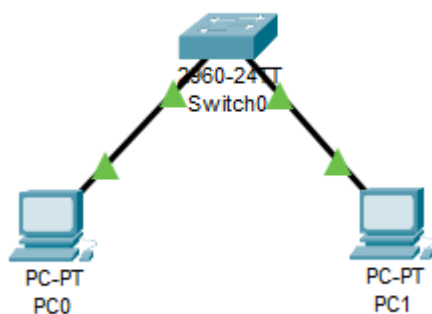


Figura 2: Escenario 1



## Escenario 1

### **Modo realtime**

En esta primera parte veremos cómo configurar una red de dos equipos conectados directamente a través de un switch.

El simulador consta de 2 modos: realtime y simulación (ver componente número 6 en la tabla 1). Para este primer apartado nos centraremos en el modo *realtime*.

Desde la caja de selección de tipo de dispositivos (componente número 8 en la tabla 1) seleccionaremos los *switches*. Posteriormente, entre las opciones disponibles para la selección de un componente específico (componente número 9), optaremos por un *switch* 2960-24TT. Dicho *switch*, al que llamaremos switch0, supondrá el primer dispositivo de nuestro escenario, y no configuraremos nada más en él.

A continuación, añadiremos 2 pc (pc0 y pc1) y los conectaremos con el switch0 por medio de cables de cobre. Para ello seleccionaremos *Connections* en la caja de dispositivos y haremos clic sobre *Copper Straight-Through*. Luego pincharemos sobre cada uno de los dispositivos que queramos comunicar y escogeremos la interfaz a la que se conectará el cable.

Se utilizará para el direccionamiento IP de esta primera parte del tutorial una dirección de clase C, 192.168.10.0/24, para asignar direcciones a todos los equipos del escenario. De acuerdo con esta información se asignarán direcciones IP y máscaras de red tanto a pc0 (192.168.10.10/24) como a pc1 (192.168.10.11/24). Para ello el simulador proporciona diferentes opciones. La opción que recomendamos es hacer clic con el botón izquierdo sobre el pc que se quiera configurar y pinchar sobre la pestaña *Desktop*, con lo cual aparecerá una ventana que se muestra en la figura 3. Finalmente, tras pulsar sobre el icono de *IP Configuration*, se especificarán los distintos parámetros de configuración de pc0.

En la figura 2 se muestra el diseño de red del escenario resultante. En la misma imagen se puede observar cómo ambos extremos de cada una de las conexiones entre el *switch* y los pc están identificados con un color. El significado de cada uno de los colores es el siguiente:

**Verde:** La interfaz física está levantada. Sin embargo, esto no es indicativo del estado del protocolo sobre la conexión.

**Verde parpadeante:** Indica que hay actividad sobre esa conexión.

**Rojo:** La interfaz física no está levantada. No se está detectando ninguna señal.

**Naranja:** El puerto está en un estado bloqueante mientras que se comprueba si existe un bucle a nivel de enlace.

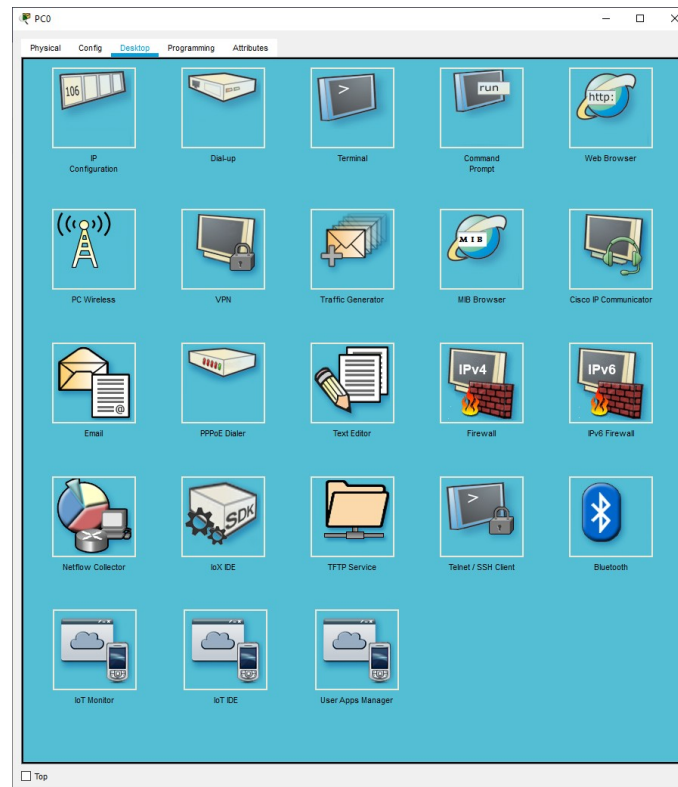


Figura 3: Pestaña de Desktop

## Modo simulación

Para comprobar que la configuración es correcta, el modo de simulación nos permite chequear el contenido de las distintas cabeceras de los datagramas enviados.

Como se puede apreciar en la figura 5, la interfaz en modo simulación consta de diferentes partes:

- **Event list:** Muestra los diferentes pasos que realizan los datagramas (permitidos por los *Event list filters*) que circulan por el escenario. Pulsando en el campo *Info* en cada fila de la lista, se muestra información más detallada acerca de cada datagrama y sus capas del modelo OSI.
- **Play controls:** Controlan la velocidad con la que los datagramas circulan por el escenario en cuestión.
- **Event list filters:** Filtran los tipos de datagramas visibles en el escenario.



- Ventana de paquetes creados en los escenarios de simulación (componente número 10 en la tabla 1): Se pueden crear escenarios con diferentes clases de datagramas. Cada escenario mostrará los datagramas enviados. En la columna *Fire* se podrán lanzar de nuevo dichos datagramas (tanto en modo simulación como en modo *realtime*). Dichos datagramas también pueden ser modificados (columna *edit*) o eliminados (columna *delete*).

Una vez configurados los tres dispositivos de nuestro primer escenario, el siguiente paso es comprobar si puede existir comunicación IP entre los dos pcs, o, lo que es lo mismo, probar si pc1 es alcanzable desde pc0 y viceversa. Para poder lograrlo, disponemos de una herramienta llamada *ping*, que se basa en dos paquetes (una petición y una respuesta) ICMP, un protocolo que se usa para el envío de mensajes de control y de error.

Se puede enviar un *ping* (en cualquiera de los dos modos) de diferentes maneras. En la forma más sencilla, es suficiente con pulsar sobre el icono en forma de sobre que aparece en la figura 4, y después hacer un clic en el dispositivo origen y un segundo clic en el dispositivo destino. El estado del datagrama en la ventana de paquetes creados determinará si el *ping* ha llegado exitosamente o si, por el contrario, ha habido algún fallo en la comunicación.

Ayudándose del modo de simulación, intentar explicar qué sucede exactamente en los siguientes casos, indicando el tipo de datagramas capturados:

- Enviamos un ping de pc0 a pc1.
- Si asignamos a pc0 la IP 192.168.6.10/24 y enviamos un *ping* desde pc0 a pc1 (192.168.10.11).
- Si asignamos a pc0 la IP 192.168.10.10/24 y enviamos un *ping* desde pc0 a 192.168.10.20.
- ¿Qué sucede si asignamos a pc0 la IP 192.168.10.10/24 y enviamos un *ping* desde pc0 a 192.168.30.20?



Figura 4: Enviar ping

The screenshot displays a network simulation environment. The main workspace shows a topology with a central switch labeled 'Switch0' connected to two PCs, 'PC0' and 'PC1'. A red envelope icon is visible near PC0. On the right, the 'Simulation Panel' is open, showing an 'Event List' table. The table has columns for 'Vis.', 'Time(sec)', 'Last Device', 'At Device', and 'Type'. The events listed are:

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC0	ICMP
	0.001	PC0	Switch0	ICMP
	0.002	Switch0	PC1	ICMP
	0.003	PC1	Switch0	ICMP
	0.004	Switch0	PC0	ICMP

Below the event list, there are controls for 'Reset Simulation', 'Constant Delay' (checked), and 'Captured to: 0.004 s'. There are also 'Play Controls' buttons (stop, play, next) and a progress bar. At the bottom, there is a status bar with 'Scenario 0' and a table of event details:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC1	ICMP		0.000	N	0	(edit)	(delete)

Figura 5: Modo simulación



## Escenario 2

A partir del escenario 1, se construirá un nuevo escenario introduciendo dispositivos de tal manera que se corresponda con el que aparece en la figura 6.

En este nuevo escenario introduciremos 1 *switch1* y 2 servidores (un servidor web y un servidor DNS). La configuración de red de estos servidores se realizará del mismo modo que se ha hecho con pc0 y pc1.

La otra novedad es la introducción de un cable de cobre cruzado entre los dos *switches* (seleccionaremos *Connections* en la caja de dispositivos y haremos clic sobre *Copper Cross-Over*). El cable es cruzado puesto que se trata de dispositivos que trabajan en un mismo nivel de la capa OSI. También se usa cable cruzado cuando los dispositivos que se conectan trabajan en capas no contiguas (un pc y un router, por ejemplo). Sin embargo, actualmente la mayor parte de dispositivos son capaces de detectar automáticamente el tipo de conexión de cable requerida y configurarla, por lo que sería posible conectar ambos *switches* sin necesidad de un cable cruzado. Si en lugar de usar el modelo 2960 usamos un modelo anterior (2950T), los *switches* no se podrían unir por medio de un cable directo y necesitaríamos el cruzado.

Para configurar cualquiera de los servidores, haremos clic izquierdo sobre ellos y pulsaremos en la pestaña *Services*. A continuación, en función del tipo de servidor, usaremos la opción HTTP o DNS.

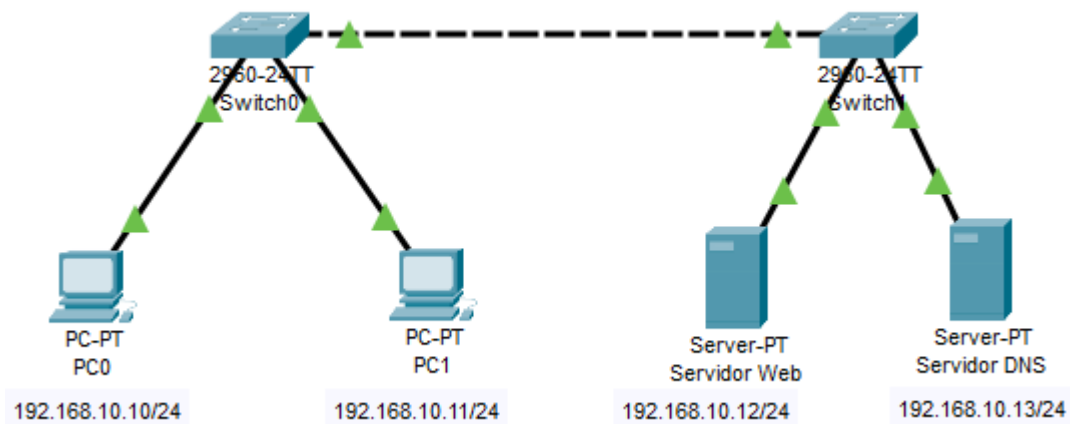


Figura 6: Escenario 2





## Servidor web

Tal y como se aprecia en la figura 7, la configuración del servicio HTTP en este caso es muy sencilla. Únicamente se permite activar o desactivar el servicio y crear páginas para luego servirlos.

Tarea: Crear una nueva página html. En ella deberá aparecer (con diferentes formatos de fuente) el nombre completo, el grupo y el horario de prácticas del alumno. Además, figurará también en esa misma página un enlace a index.html.

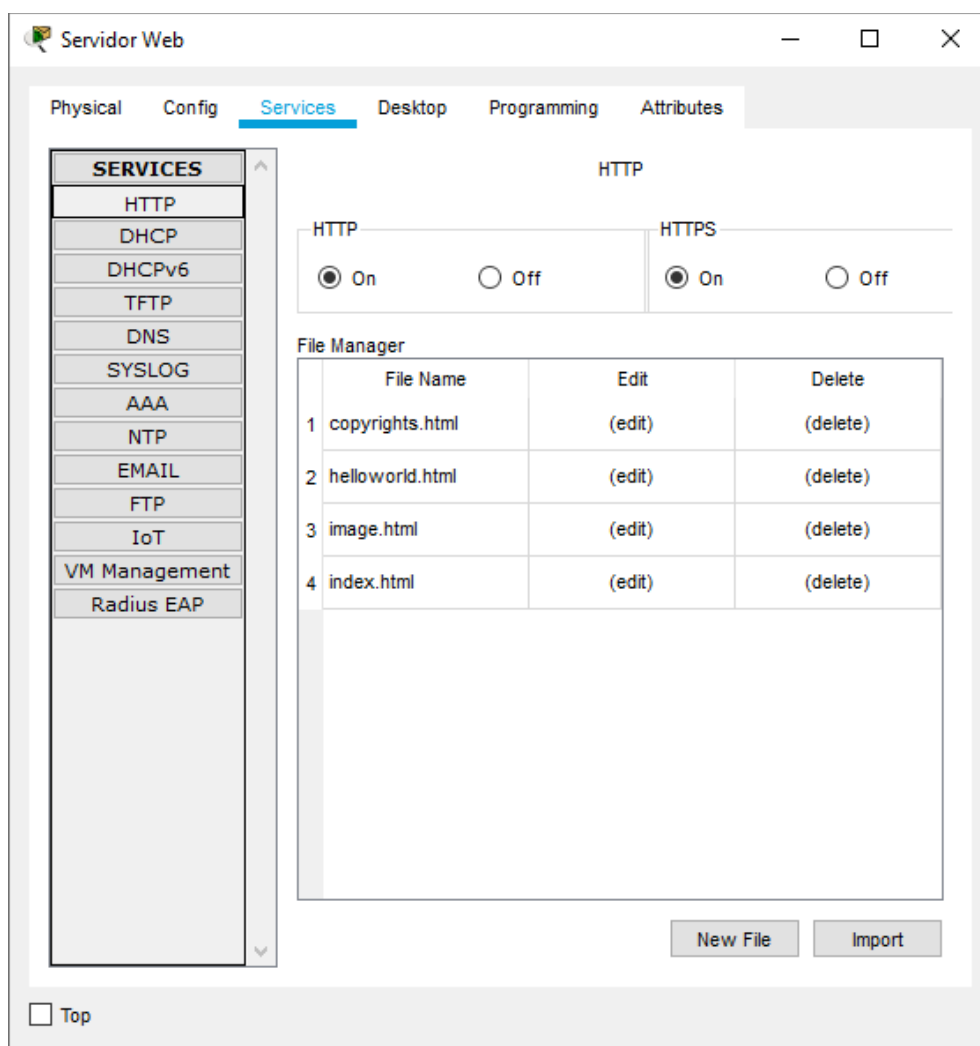


Figura 7: Servidor web



## Servidor DNS

Como se muestra en la figura 8, el servidor DNS aparece, por defecto, desactivado.

Tareas: Activar el servicio y añadir un nuevo registro tipo A, con nombre [www.redes.fic.com](http://www.redes.fic.com) y la IP del servidor web. A continuación, hacer clic izquierdo sobre cada uno de los PC y en la pestaña *Desktop* configurar la IP adecuada para el servidor DNS pinchando sobre el icono *IP Configuration*. Finalmente, comprobar que la resolución se realiza correctamente empleando, por ejemplo, el comando *nslookup* desde el *Command Prompt*.

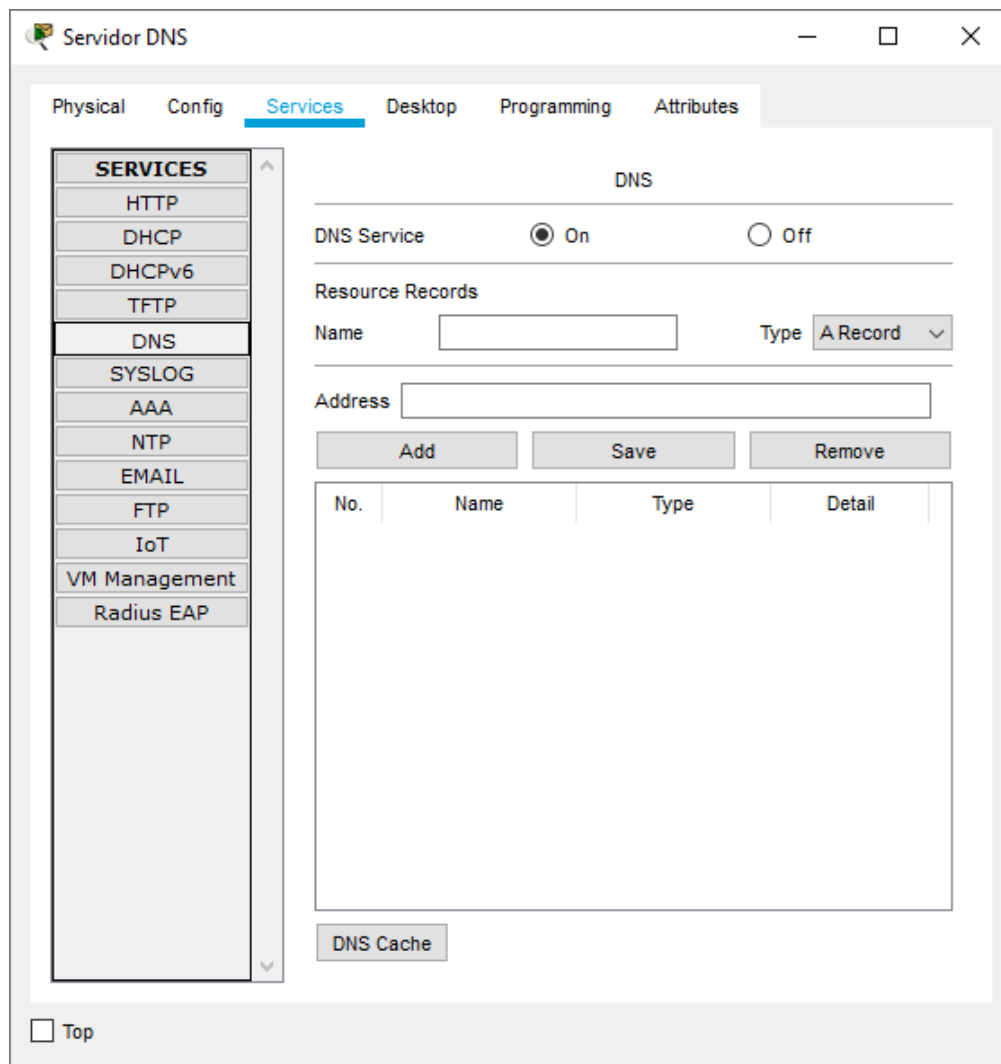


Figura 8: Servidor DNS



## ***Ejercicios sobre el escenario 2***

- ¿Cuál es la IP del switch 0? ¿y la del switch 1?
- ¿Cómo te conectarías al servidor web por IP? ¿y por nombre?
- Haciendo una petición HTTP al servidor web desde pc0, ¿cuál es el puerto TCP que usa pc0 para esa comunicación? ¿y el servidor web?
- ¿Cómo se añadiría una nueva página HTML con un enlace a index.html en el servidor web?
- ¿Qué pasa si desconecto el servidor DNS y en el navegador de pc0 me conecto a 192.168.10.12? ¿y si me conecto a www.redes.fic.com?
- Establecer la dirección del servidor DNS a 192.168.20.13 y modificar pc1 según esta nueva configuración. ¿Qué sucede si accedemos desde pc1 a <http://www.redes.fic.com>? ¿y si nos conectamos a <http://192.168.10.12>?



## Escenario 3

El escenario 3 (ver figura 9) introduce un nuevo dispositivo: el *router*. Partiremos del escenario 2 para conseguir este nuevo escenario.

Primero se configurarán las interfaces de los 2 pc y de los servidores, con las IP que aparecen en la figura 9.

Después se le asignará una IP a cada una de las interfaces de los *routers*. Para ello, se hace clic izquierdo sobre el *router*, se va a la pestaña *Config* y se pulsa sobre la interfaz a configurar. Luego, se le asigna la IP y la máscara y se levanta la interfaz activando el *checkbox* de *Port Status*, tal y como se muestra en la figura 10.

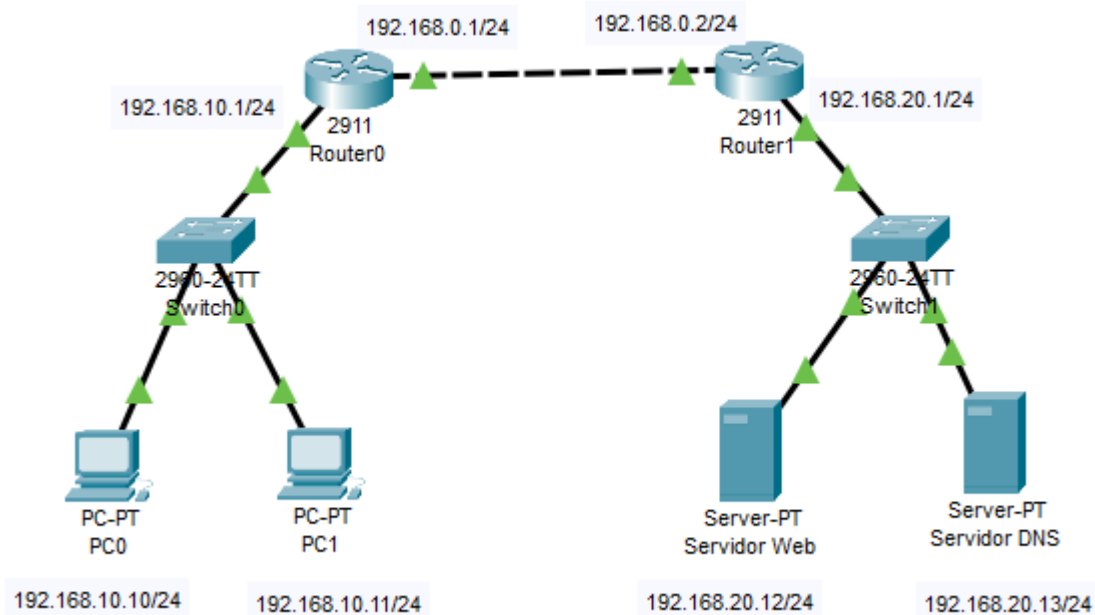


Figura 9: Escenario 3



The screenshot shows the 'Router0' configuration window with the 'Config' tab selected. The left sidebar lists various configuration categories: GLOBAL, ROUTING, SWITCHING, and INTERFACE. Under the 'INTERFACE' category, 'GigabitEthernet0/0' is selected. The main panel displays the configuration for 'GigabitEthernet0/0', including Port Status (On), Bandwidth (1000 Mbps), Duplex (Half Duplex), MAC Address (0030.A391.1B01), IP Configuration (IP Address and Subnet Mask fields), and Tx Ring Limit (10). Below the configuration fields, there is a section for 'Equivalent IOS Commands' showing the following commands:

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
```

Figura 10: Configuración de interfaz del router

The screenshot shows the 'Router0' configuration window with the 'Config' tab selected. The left sidebar lists various configuration categories: GLOBAL, ROUTING, SWITCHING, and INTERFACE. Under the 'ROUTING' category, 'Static' is selected. The main panel displays the 'Static Routes' configuration section, which includes fields for Network, Mask, and Next Hop, followed by an 'Add' button. Below this, there is a 'Network Address' field and a 'Remove' button. At the bottom, the 'Equivalent IOS Commands' section shows the following commands:

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#
```

Figura 11: Configuración de rutas estáticas



Una vez completados los pasos anteriores se pide que se responda a las siguientes preguntas:

- ¿Qué sucede al hacer un *ping* de pc0 a pc1?
- ¿Qué sucede al hacer un *ping* desde el servidor web al servidor DNS? ¿y al hacerlo desde el servidor web al router1? Si alguno de ellos falla, intenta solucionar el problema.
- ¿Qué sucede al hacer un *ping* de pc0 al *router1*? ¿y del servidor web al *router0*? ¿por qué?

A continuación, se configurarán las rutas necesarias en los 2 routers. Para ello basta con hacer clic izquierdo en cada uno de ellos y acceder a la pestaña que se muestra en la figura 11. Hay que tener en cuenta que la entrada en la tabla de enrutamiento para la dirección de *loopback*, así como las entradas para las redes directamente conectadas, son automáticamente creadas al levantar la interfaz, por lo que no han de ser explícitamente introducidas.

Hacer un *ping* desde pc0 al servidor web y usar el modo simulación para contestar a:

- ¿Qué IP de origen tiene el datagrama IP al salir de pc0? ¿y al salir de router0? ¿qué ha sucedido en *router0* con respecto a las direcciones de la cabecera IP? ¿por qué?
- Desde el *Web Browser* de pc1 (ver figura 3), hacer una petición a <http://www.redes.fic.com>. Teniendo en cuenta los protocolos vistos hasta ahora en la asignatura, explicar el proceso completo hasta recibir la respuesta HTTP en pc1 ayudándose de nuevo del modo simulación. ¿Qué ocurre si la petición se envía a <http://192.168.20.12>? ¿qué respuesta se obtiene?



## ARP

Address Resolution Protocol (ARP) es un protocolo de nivel de enlace que proporciona la correspondencia entre direcciones MAC y direcciones IP. Para eso sigue un modelo petición-respuesta:

1. En primer lugar, el dispositivo que necesita conocer la correspondencia envía una petición de broadcast a la red preguntando qué dirección MAC se corresponde con la dirección IP que figura en la petición.
2. En caso de que exista el dispositivo con esa IP en el segmento de red, dicho dispositivo responderá con una trama unicast indicando cuál es la dirección MAC que se corresponde con la dirección IP solicitada.

Para no tener que enviar continuamente este tipo de peticiones, los dispositivos disponen de cachés ARP en donde almacenan estas correspondencias. Para poder ver el contenido de estas cachés existen distintas alternativas, entre las que destacamos:

1. En el Command Prompt de pc0 accesible desde la pestaña de Desktop (ver Figura 3), ejecutar el comando *arp -a*.
2. Con la herramienta *Inspect*, la lupa disponible en la *barra de tareas comunes* (componente 3 en la Figura 1), hacer clic en un router y escoger la opción *ARP Table*.

Tras haber hecho pruebas, probablemente estas cachés no estarán vacías.

En modo simulación, visualizando únicamente el tráfico ICMP y ARP (ver sección de comentarios útiles), enviar un ping de pc0 al servidor Web. En esta primera prueba es muy probable que no se muestren las tramas ARP, puesto que las correspondencias necesarias ya figurarán en las cachés.

A continuación, cambiar la IP del Servidor Web (192.168.20.14), modificar la tabla de enrutamiento de R0 indicando como next hop 192.168.0.3 para la red 192.168.20.0, y cambiar la IP de la interfaz 192.168.0.2 de R1 y usar 192.168.0.3. Acto seguido, enviar de nuevo el ping. ¿Qué sucede ahora? ¿qué tramas circulan por los segmentos de red para que el ICMP echo reply pueda alcanzar finalmente a pc0? (repetir el envío del ping en caso de que sea necesario).

Cubrir la siguiente tabla considerando que pc0 y Router0 se acaban de reiniciar (tienen las cachés ARP vacías), mientras que el Servidor Web y Router1 disponen de las entradas necesarias en sus cachés ARP. Para cubrir la tabla no es necesario replicar el estado inicial de las cachés ARP en el escenario (llega con entender el tráfico que se enviaría).

Indicar la siguiente información para cada una de las tramas obtenidas:



- Segmento de red (LAN 0, LAN 10 o LAN 20 en función del tercer octeto de la dirección de red).
- En la cabecera de enlace: origen, destino, tipo de mensaje.
- En la cabecera de red o en la trama ARP: IP origen, IP destino, protocolo (IP/ARP).
- Mensaje encapsulado.

LAN	Enlace			IP/ARP			Mensaje
	Origen	Destino	Tipo	IP origen	IP destino	Protocolo	
10							ARP req
10							ARP resp
10							Echo req
0							ARP req
0							ARP resp
10							Echo req
0							Echo req
20							Echo req
20							Echo resp
0							Echo resp
10							Echo resp





## Comentarios útiles

- A la hora de capturar tráfico en el modo simulación es muy recomendable que en los filtros de la lista de eventos no estén marcados los siguientes protocolos: CDP, DTP, STP y VTP. Éstos generan mucho tráfico que se escapa del contenido de la asignatura.
- Pinchando en el menú *Options*, y a continuación sobre *Preferences*, existen varias opciones muy útiles para la realización de prácticas. Entre ellas destacaremos dos:
  - En la pestaña *Interface*, marcar la opción *Always Show Port Labels* permitirá mostrar a qué interfaces de los dispositivos están conectados los cables del escenario.
  - En la pestaña *Miscellaneous*, recomendamos que se active la opción *Buffer Filtered Events Only*, disponible sólo en versiones recientes del software (a partir de la 6.1.1.001). Así, en modo simulación no habrá problemas con el llenado del buffer, siempre y cuando se desmarquen los protocolos del punto anterior.
- Pulsando la tecla *CTRL* a la vez que se hace clic sobre cualquier icono de la caja de selección de dispositivo específico, se puede introducir en el escenario más de un dispositivo del mismo modelo sin necesidad de hacer clic varias veces sobre el icono. Para dejar de introducir dispositivos se pulsa la tecla *Escape*.
- En la barra de tareas comunes, hay un icono de una lupa. Es herramienta es muy práctica para ver, por ejemplo, tablas de enrutamiento.
- En modo *realtime*, para que la red converja rápido (es decir, para que las luces de los puertos se pongan en verde antes), es útil pulsar sobre *Fast Forward Time*, botón situado en la barra de *realtime*.



## **Evaluación**

Para la evaluación de este tutorial se empleará el cuestionario “Cuestionario: Tutorial de Packet Tracer / Questionnaire: Packet Tracer Tutorial” de Moodle. La fecha límite para cubrir el cuestionario es el 8 de abril de 2022 a las 23:59. La nota máxima será de 0,25 puntos.